RIKER
DANZIG
SCHERER
HYLAND
PERRETTI LLP

CYBER SECURITY & DATA PRIVACY

Riker Danzig Scherer Hyland & Perretti LLP is one of New Jersey's oldest and largest law firms. Utilizing its strengths in litigation, government affairs, and risk counseling, Riker Danzig has helped clients who encounter the legal difficulties presented by cyberattacks, loss of electronic data, mistakes in electronic fund transfers, and other computer-related issues.

The Firm has found that cyber issues often require a multi-disciplinary approach to contain and mitigate risk. It is essential that legal counsel coordinate the resources of a company's technology experts, financial personnel, and executives to ensure that a cyber or technology problem has been addressed appropriately and efficiently, with a sensitivity to the privacy, regulatory, and liability exposures that these issues present. We are able to draw on attorneys from our practice groups who specialize in litigation, insurance, white collar crime, transactions, government affairs, intellectual property, and technology and emerging growth companies, to find workable and business savvy solutions for cyber-related problems.

Our experience in this area has ranged from involvement in the legal aftermath of some of the world's largest and most notable cyberattacks, to counseling clients during and immediately after sensitive electronic security breaches. The following examples help illustrate our experience in this rapidly evolving and growing area.

- We were retained by a domestic insurance company to investigate and evaluate a series of claims presented by its insured relating to high-profile cyberattacks. The attacks involved significant and repeated data security breaches affecting a widely used video game system, which shut down the insured's networks for extensive periods of time, resulting in significant business interruptions and the potential compromise of confidential and personal information of thousands of network users. We worked with the insured's defense team on various technical issues, and monitored and provided advice with respect to various issues that arose in the ensuing consumer class action litigation.
- We were retained by a domestic insurance company to provide advice with respect to a notorious cyberattack on a well-known film and entertainment company, which resulted in physical damage to its network, the theft of confidential and personal information of the insured's employees and vendors, the illegal pirating of five unreleased motion pictures, and threats of terrorism. As counsel for the insured's lead

insurer, we coordinated with a team of forensic cyber-security and accounting experts to investigate these cyberattacks and the exposures they presented.

- We were retained by a title insurance company in connection with a scheme by a hacker who succeeded in having funds from a real estate transaction wired into his account. International hackers compromised the email account of the seller's attorney in a significant real estate transaction and, using an email address similar but not identical to the seller's attorney's address, misdirected the entire sales proceeds to the hacker's account instead of the intended seller's attorney's account. We have filed suit against various parties to the sales transaction to determine ultimate liability, raising novel issues concerning responsibility for the accuracy of wiring instructions.
- We currently provide legal guidance to a domestic insurance services provider concerning its compliance obligations under 23 NYCRR 500, a "first-in-the-nation" cybersecurity regulation recently adopted by the New York State Department of Financial Services in March 2017. The regulation requires banks, insurance companies and other financial service institutions to conduct periodic risk assessments and to implement and maintain responsive, comprehensive cybersecurity programs and policies to ensure the mitigation of cybersecurity risks and the protection of consumers' data. In addition to providing legal advice, we are preparing a plan of action for the client and coordinating with various IT experts, risk assessment vendors and other technical service providers to ensure its compliance with the new regulation.
- We were retained by a domestic insurer to investigate and analyze a claim for damage to an insured in connection with an electronic theft by the insured's former employee who allegedly stole the insured's proprietary information and trade secrets regarding a purported new technology for the defense industry.
- We were retained by an international insurance company to provide advice concerning the question of whether cyber liability coverage is subject to the Terrorism Risk Insurance Act ("TRIA"), which Act requires insurers to make available terrorism risk insurance in connection with property and casualty insurance policies. This question is significant, because an insurer's failure to comply with TRIA requirements could jeopardize its eligibility for reimbursement under the TRIA program. We reviewed the U.S. Department of Treasury's recent guidance, as well as TRIA's implementing regulations, to determine how cyber coverage would be treated under TRIA to ensure our client's continued compliance with the program.
- We were retained by a domestic insurer to analyze coverage for multiple claims made against an insured stemming from a data breach that resulted in the disclosure of personal and confidential financial consumer information belonging to approximately 23,000 individuals. We successfully negotiated a settlement with the underlying claimants that included a substantial contribution from another insurer whose policy specifically covered such claims.
- We represented a domestic insurer and successfully obtained injunctive relief against an individual for his "cyber assault" on the insurer. Specifically, we filed an order to show cause under the Anticybersquatting Consumer Protection Act and obtained an order immediately and permanently restraining the individual

from publishing false and misleading information about the company on several websites that he operated, requiring him to cease the unauthorized use of the company's logo, and to cease sending harassing email correspondence to the company's board of directors and chief executive officer.